Sensor networks security based on sensitive robots agents. A conceptual model

Camelia-M. Pintea[a], Petrica C. Pop[a]

[a] *Technical University Cluj Napoca, North University Center Baia Mare, Romania*

Abstract

Multi-agent systems are currently applied to solve complex problems. The security of networks is an eloquent example of a complex and difficult problem. A new model-concept *Hybrid Sensitive Robot Metaheuristic* for *Intrusion Detection* is introduced in the current paper. The proposed technique could be used with machine learning based intrusion detection techniques. The new model uses the reaction of virtual sensitive robots to different stigmergic variables in order to keep the tracks of the intruders when securing a sensor network.

Keywords: intrusion detection, sensor network, intelligent agents

1. Introduction

Prevention and detection of intruders in a secure network is nowadays a challenging issue. The intrusion detection system based on computational intelligence (*CI*) has proved in time to have huge advantages over traditional detection systems due to characteristics of *CI* methods: adaptation, fault tolerance, high computational speed etc. It is essential to design efficient *Intrusion Detection Systems (IDS)* especially for open medium networks as wireless sensor devices.

The intrusions could be missue intrusions and anomaly intrusions. Missue intrusions are the attacks knowing the weak points of a system. Anomaly intrusions are based on observations of normal system usage patterns and detecting deviations from the given norm. The mentioned intrusions are hard to quantify because there are no fixed patterns that can be monitored and as a result a more fuzzy approach is often required.

The *Intrusion Preventing Systems (IPS)* are network security appliances that monitor network and/or system activities for malicious activities. *IPS* is a device used to block all the unwanted access to the targeted host, to remove malicious part of packets and as well it may reconfigure the network device where an attack is detected [3].

Social autonomic cooperative colonies as ants, bees and others have the capability to coordinate and construct complex systems [4]. Using their behavior, engineers have built real collective robotic systems. The metaheuristics based on classes of specialized robots provide feasible solutions for nowadays complex problems. One of these techniques is *Sensitive Robot Metaheuristic* developed by Pintea et al. [19, 21]. The sensitive model was introduced and explained in [5, 6, 21] and used to solve complex problems in [7, 20, 21]. The *SRM* model was implemented first to solve a large drilling problem but it has the potential to solve other *NP*-hard problems including intrusion detection. The model ensure a balance between diversification and intensification in searching.

The aim of the current paper is to provide an effective stigmergic-based technique for *IDS* in a sensor network graph, that consist of multiple detection stations called sensor nodes. The new *Hybrid Sensitive Robot Metaheuristic for Intrusion Detection (HSRM-ID)* model uses a collection of robots endowed with a stigmergic sensitivity level. The sensitivity of robots allow them to detect and react to different stigmergic variables involving the attacks into a secure network. The hybrid model combines elements from *Sensitive Robot Metaheuristic (SRM)* [19] as *Ant Colony System (ACS)* [10], autonomous mobile robots and the intrusion detection based on emotional ants for sensors *(IDEAS)* [2].

2. Sensitive Stigmergic Robots

The metaheuristic *Sensitive Robot Metaheuristic (SRM)* [19] combining the concepts of stigmergic communication and autonomous robot search is used to solve *NP*-hard optimization problems. The basic concepts are defined and described further in this section, see for more details [4, 5, 6, 7, 19, 20, 21].

Definition 1. *Stigmergy occurs when an action of an insect is determined or influenced by the consequences of the previous action of another insect.*

Definition 2. *Sensitive robots refers to artificial entities with a Stigmergic Sensitivity Level (SSL) expressed by a real number in the unit interval [0, 1].*

Email addresses: cmpintea@yahoo.com (Camelia-M. Pintea), petrica.pop@ubm.ro (Petrica C. Pop)

Definition 3. *Environment explorers'robots are sensitive robots with small Stigmergic Sensitivity Level (sSSL) with the potential to autonomously discover new promising regions of the search space.*

Definition 4. *Environment exploiters robots are sensitive robots with high Stigmergic Sensitivity Level (hSSL) emphasizing search intensification.*

An important characteristic of stigmery is that individual behavior modifies the environment, which in turn modifies the behavior of other individuals [11]. The *SRM* technique attempts to address the coupling between perception and action as direct as possible in an intelligent stigmergic manner.

As it is known, *robot communication* relies on local environmental modifications that can trigger specific actions. The set of the rules defining actions (stimuli pairs) used by a homogeneous group of stigmergic robots defines their behavior and determines the type of structure the robots will create [4, 26]. Robot stigmergic communication does not rely on chemical deposition as it is for artificial ant-based colonies [10]. A stigmergic robot action is determined by the environmental modifications caused by prior actions of other robots. The value of quantitative stigmergy modify the future actions of robots. Discrete stimulus are involved in qualitative stigmergy and the action is switched to a different action [4, 26].

Some real-life applications of the behavior-based approach, including autonomous robots, are in data mining, military applications, industry and agriculture, waste management, health care.

3. Intrusion detection techniques using Artificial Intelligence

At first are introduced the main concepts of *IDS* followed by a survey of *Artificial Intelligence*-based existing models for computer security.

3.1. Intrusion Detection System

Due to increasing incidents of computer attacks, it is essential to build efficient intrusion detection mechanisms. The definitions of the main concepts related to this domain are given in what it follows, see for example [8, 13].

Definition 5. *Intrusion detection technology is a technology designed to monitor computer activities for the purpose of finding security violations.*

Definition 6. *Intrusion detection system (IDS) is a system that implements intrusion detection technology.*

Definition 7. *A security violation of a system is any deliberate activity that is not wanted including denial of service attacks, port scans, gaining of system administrator access and exploiting system security holes.*

Definition 8. *Intrusion Prevention System (IPS) is active, in-line device in the network that can drop packets or stop malicious connection before reaching the targeted system.*

IPS is able to detect and prevent attacks but it has not deeper detection capabilities of *IDS*. Neither of *Intrusion Detecting System* and *Intrusion Prevention System* is capable to provide in depth security. *Intrusion Detecting and Prevention System (IDPS)*, a combinations of *IDS* and *IPS*, is a more effective system capable of detection and prevention [22]. Based on the placement, the *IDPS* is divided into four classes as follows:

1. a *network-based system*, which is able to monitor traffic of network or its particular segment and identify different network attacks.

   An example of network-based system is Snort [14]. *Snort* is an open source network intrusion prevention and detection system - nowadays a standard for IPS - that combines the benefits of signature, protocol and anomaly-based inspection. A number of problems associated with *Network-based system* according to [17] are:

   – they cannot fully detect novel attacks;
   – variations of known attacks are not fully detected;
   – they generate a large amount of alerts, as well as a large number of false alerts;
   – the existing *IDS* is focus on low-level attacks or anomalies and do not identify logical steps or strategies behind these attacks.

2. *host-based systems* describe the class of software able to monitor a single system, analyse characteristics and log to at one host. These systems are deployed on critical hosts.

3. *wireless-based systems* analyse wireless traffic to monitor intrusion or any suspicious activity. They scan traffic but are not able to identify attack in the application layer or higher layer network protocols as UDP and TCP. It may be deployed at the point where unauthorized wireless network could be accessed.

4. *behavior-based systems* are used for examining network traffic in order to identify attacks (e.g. Denial of Service attacks). These systems are deployed to monitor flow of network or flow between internal and external network.

3.2. Artificial Intelligence in Intrusion Detection System

The current paper deals with an artificial intelligent approach for intrusion detections. A short review of the main *AI* techniques already used and their benefits for detecting intrusion in network systems follows.

According to Beg et al. [3], the intrusion detection classical algorithms have the following disadvantages: false alarm rate and constant updates of database with new signatures. The network administrator responds to alarms and updates the signatures that increases in time. For example, in the already mentioned *Snort* signatures increased from 1500 to 2800 over two years [14]. In order to improve the administrator work, reducing the number of false alarms and better intrusion detection are introduced artificial intelligence mechanisms [23]. Some of AI techniques used in intrusion detection are data mining, genetic algorithm, neural network, multi-agents, ant-net miner, etc.

Lee et al. [15] introduced a data mining classification mechanism with association rules from the audit data - knowledge present in a knowledge base - providing gaudiness for data gathering and feature selection. In order to detect abnormal behavior one can use genetic algorithms, see for example [1]. In [18], neural networks use back propagation *MLP* for a small network in order to detect anomalies and identify user profiles after end of each log session.

It shall also be remarked that several of the leading methods for detecting intrusions and detecting intrusions are hybrid artificial approaches, which combine different AI solution techniques [9, 16, 25]. Some hybrid methods used in the literature are data mining and fuzzy logic techniques [16], data mining and genetic algorithm selecting the best rules for the system [9]. In the future could be implemented hybrid models involving intelligent evolutionary agents [12] and dynamic decision boundary using Support Vector Machine [24] for handle a large number of features.

Banerjee et al. [2] introduced an intrusion detection based on emotional ants for sensors *(IDEAS)*, which could keep track of the intruder trials. This technique is able to work in conjunction with the conventional machine learning based intrusion detection techniques to secure the sensor networks.

4. Hybrid Sensitive Robot Metaheuristic for Intrusion Detection

In this section we introduce a new hybrid metaheuristic in order to detect the intruders in a sensor network. The new model is called *Hybrid Sensitive Robot Metaheuristic* for *Intrusion Detection (HSRM-ID)*, is based on *Sensitive Robot Metaheuristic (SRM)* introduced in [19] and uses a specific rule in order to generate a state of thinking or the choice of an intruder [2].

The proposed *(HSRM)* can be modelled using two distinct groups of sensitive stigmergic robots. The first group of robots-agents is endowed with small sensitive values *SSL* and they are sensitive-explorers (*sSSL: small SSL-robots*). They can sustain diversification in intruders searching. In the second group are the robots-agents with high sensitive stigmergic values (*hSSL: high SSL-robots*). They are sensitive-exploiters and could exploit intensively the regions already identified with attacks from intruders. In time, based on the experience of robots-agents, the sensitive stigmergic level *SSL* can increase or decrease.

The pseudo-code description of the *Hybrid Sensitive Robot Metaheuristic* for *Intrusion Detection* is described in what it follows.

Algorithm 1 Hybrid Sensitive Robot Algorithm for Intrusion Detection

```
Set parameters; initialize stigmergic values of the trails;
for k=1 to m do
    Place robot k on a randomly chosen node of a sensor network;
    for i=1 to Niter do
        Each robot incrementally builds a solution based on the autonomous search sensitivity;
        The sSSL robots choose the next node based on the attack probability (1);
        A hSSL-robot uses the information supplied by the sSSL robots to chose the new node (2);
        Apply a local stigmergic updating rule (3);
        Apply the rule generating a state of thinking or the choice of an intruder (4):
        A global updating rule is applied (5);
        Validate the path and detect intruder;
    end for
end for
```

The stigmergic value of an edge is τ and the visibility value is η. A *tabu list* with the already visited nodes is maintained, see [10] for more details. In order to divide the colony of m robots in two groups it is used a random variable uniformly distributed over $[0, 1]$.
Let q be a realization of this random variable and q_0 a constant $0 \leq q_0 \leq 1$. If the inequality $q > q_0$ stands the robots are endowed with small sensitive stigmergic value *sSSL* robots and otherwise they are highly sensitive stigmergic robots (*hSSL*). A *hSSL-robot* uses the information supplied by the *sSSL* robots.

In order to define the rule to generate a state of thinking or the choice of an intruder we use the same notations as in Banerjee et al. [2]:

- $A(I, s, t)$ denotes the tendency of an intruder I to be assigned to the sensor node s at moment t.
- $I_1(intruder1)\_C(I, s, t)$ is the potential to generate the state of choice to a particular path in the network sensor graph.
- $I\_C(I, s, t)$ is the intensity of the attack,
- $f\_C(.)$ is a function specific of the thinking of intruder
- $T\_c(I, t)$ is the threshold value.

The new hybrid model *(HSRM-ID)* for identifying the affected path of a sensor network graph is described further.

- Initially the *SSL* robots are placed randomly in the network space. The parameters of the algorithm are initialized.

- A *SSL* robot chooses the next move with a probability based on the distance to the candidate node and the stigmergic intensity on the connecting edge. In order to stop the stigmergic intensity increasing unbounded each time unit evaporation takes place.

- Let i be the current node. The next node is chosen probabilistically. Let $J^k{}_i$ be the unvisited successors of node i by robot k and $u \in J^k{}_i$. As in *Ant Colony System* technique [10] the probability of choosing the next node u, possible to be attacked, is shown in (1).

$$p^k{}_{iu}(t) = \frac{[\tau_{iu}(t)][\eta_{iu}(t)]^\beta}{\Sigma_{o \in J^k{}_i}[\tau_{io}(t)][\eta_{io}(t)]^\beta}, \qquad (1)$$

  where β is a positive parameter, $\tau_{iu}(t)$ is the stigmergic intensity and $\eta_{iu}(t)$ is the inverse of the distance on edge (i, u) at moment t.

- The new node j is choose by *hSSL* robots using (2):

$$j = argmax_{u \in J_i^k}\{\tau_{iu}(t)[\eta_{iu}(t)]^\beta\}, \qquad (2)$$

  where β determines the relative importance of stigmergy versus heuristic information.

- Update trail stigmergic intensity by local stigmergic rule (3):

$$\tau_{ij}(t+1) = q_0^2 \tau_{ij}(t) + (1 - q_0)^2 \cdot \tau_0. \qquad (3)$$

  where (i, j) are the edges belonging to the most successful traversing across sensor nodes.

- Equation (4) illustrates the rule to generate a state of thinking or the choice of an intruder [2].

$$\begin{aligned} &\text{If } I\_C(I,s,t) = I\_C(I,s,t) - T\_C(I,t) \\ &\qquad \text{then } l\_C(l,s,t) > I\_C(l,t) \\ &\qquad\qquad \text{else } I\_C(I,s,t) = 0. \end{aligned} \qquad (4)$$

- A global updating rule is applied [2] as in (5) and is used a tabu list where to store the track and edge details.

$$\tau_{ij}(t+1) = q_0^2 \tau_{ij}(t) + (1 - q_0)^2 \cdot \sum_{j=1}^{k} \Delta s^j \tau_{ij}(t), \qquad (5)$$

  where

$$\Delta s^j t_{ij} = \begin{cases} f(s^j) & \text{if } s^j \text{ contributes to } \tau_{ij} \\ 0 & \text{otherwise} \end{cases} \qquad (6)$$

  and where q_0 is the evaporation rate, $\Delta s^j \tau_{ij}$ is the combination of a solution s^j with the update for pheromone value τij; $f(s^j)$ is the function specific to the thinking of the intruder and k is the number of solution used for updating the pheromones.

Table 1: Analyze the action of agents-robots based on the pheromone level on the edges of the sensor network graph.

Agents	Intruders searching type	Pheromone Level	Detecting intrusion	Action Type
sSSL robots	explorers	low	no	continue to explore
		high	possibly intruders	notify hSSL robots
hSSL robots	exploiters	low	the attack is not certified	update pheromone trails
		high	attack is highly present	identify affected path

- Update the intensity of attack value $I\_C(I, s, t)$ through validating the path and detect intruder.

The output of the algorithm is the most affected path of a sensor network with n nodes. Termination criteria is given by the number of iterations, denoted by N_{iter}. The complexity of the proposed algorithm is $O(n^2 \cdot m \cdot N_{iter})$.

5. The analyze of the new concept

In the following is performed an analyze of the *Hybrid Sensitive Robot Algorithm for Intrusion Detection.* The artificial pheromone from the edges of the sensor network graph reveals as the attacked zone within the network. Each bio-inspired robot uses his one specific properties as his level of sensitivity in order to detect the intruders and the artificial stigmergy in order to find the attacked edges. Table 1 illustrates the behavior of different groups of sensitive bio-inspired virtual robots when investigate the sensor network in search of intrusion. As a concept, the introduced model *Hybrid Sensitive Robot Algorithm for Intrusion Detection* has more chances to improve the intrusion detection systems comparing with the existing approaches from the literature, due to the sensitivity property of the bio-inspired robots. As well the diversity of robots groups implies also different values of virtual pheromone trail values. The robots with small stigmergic value are constantly sustaining diversification in intruders searching and as a complementary action, the robots with high sensitive stigmergic values are testing the already identified networks attacked regions. In the future we will perform numerical experiments to assess the performance of the proposed algorithm.

6. Conclusions

Nowadays the networks are threatened by security attacks and resource limitations. In order to deal with this security network problem efficient intruders detection and prevention systems are used. Within this paper we introduce a new concept *Hybrid Sensitive Robot Algorithm for Intrusion Detection* based on bio-inspired robots. It is used a qualitative stigmergic mechanism, each robot is endowed with a stigmergic sensitivity level facilitating the exploration and exploitation of the search space. In the future some computational tests will be proposed and further hybrid AI techniques will be involved for securing the networks.

Acknowledgement.

This research is supported by Grant PN II TE 113/2011, New hybrid metaheuristics for solving complex network design problems, funded by CNCS Romania.

References

[1] L. Alhazzaa. Intrusion Detection Systems using Genetic Algorithms. 2007.

[2] S. Banerjee, C. Grosan and A. Abraham. IDEAS: Intrusion Detection based on Emotional Ants for Sensors. *Intelligent Systems Design and Applications.* IEEE C.S. 344–349, 2005.

[3] S. Beg, U. Naru, M. Ashraf and S. Mohsin. Feasibility of Intrusion Detection System with High Performance Computing: A Survey. *Int. J. for Advances in Computer Science.* 1(1):26–35, 2010.

[4] E. Bonabeau, M. Dorigo and G. Tehraulaz. *Swarm intelligence from natural to artificial systems.* Oxford, UK: Oxford Univ. Press, 1999.

[5] C. Chira, C-M. Pintea and D. Dumitrescu. *Sensitive stigmergic agent systems: a hybrid approach to combinatorial optimization.* Innovations in Hybrid Intelligent Systems, Advances in Soft Computing, 44:33–39, 2008.

[6] C. Chira, C-M. Pintea and D. Dumitrescu. *Cooperative learning sensitive agent system for combinatorial optimization.* NICSO 2007, Studies in Computational Intelligence, 129:347–355, 2008.

[7] C. Chira, D. Dumitrescu and C-M. Pintea. Learning sensitive stigmergic agents for solving complex problems. *Computing and Informatics*, 29(3):337–356, 2010.

[8] T. Crothers. *Implementing Intrusion Detection Systems*, Wiley, 2003.

[9] Y. Dhanalakshmi and I. R. Babu. Intrusion detection using data mining along fuzzy logic and genetic algorithms. *Int. J. of Computer Science and Network Security*, 8(2):27–32, 2008.

[10] M. Dorigo and L. M. Gambardella. Ant Colony System:A cooperative learning approach to the Traveling Salesman Problem. *IEEE Trans.Evol.Comp.* 1:53–66, 1997.

[11] Grassé, P.-P. La Reconstruction du Nid et Les Coordinations Interindividuelles Chez Bellicositermes Natalensis et Cubitermes. *Insect Soc.* 6:41–80, 1959.

[12] B. Iantovics and C. Enachescu. *Intelligent Complex Evolutionary Agent-based Systems.* Development of Intelligent and Complex Systems. AIP, 116-124, 2009.

[13] N. Ierace, C. Urrutia and R. Bassett. Intrusion Prevention Systems. *Ubiquity*, ACM, 2–2, 2005.

[14] Kim, B., Yoon, S., Oh, J. Multi-hash based Pattern Matching Mechanism for High-Performance Intrusion Detection. *Int. J. of Computers* 1(3):115–124, 2009.

[15] W. Lee, S. Stolfo and K. Mok. Mining audit data to build intrusion detection models. *Knowledge Discovery and Data Mining*, New York, AAAI Press, 66–72 (1998)

[16] J. Luo. *Integrating Fuzzy Logic and Data Mining Methods for Intrusion detection.* Master thesis, Mississippi State University, 1999.

[17] S. Northcutt. *Network Intrusion Detection.* New Riders Publishers, 2002.

[18] J. Ryan, M-J. Lin and R. Miikkulainen. Intrusion Detection with Neural Networks. *Advances in Neural Information Processing Systems* 10, MIT Press, 1998.

[19] C-M. Pintea, C. Chira, D. Dumitrescu and P.C. Pop. *A sensitive metaheuristic for solving a large optimization problem.* SOFSEM 2008, LNCS 4910, 551–559, 2008.

[20] C-M. Pintea, C. Chira and D. Dumitrescu. *Sensitive ants: Inducing diversity in colony.* NICSO 2008, Studies in Computational Intelligence, 236:15–24, 2009.

[21] C-M. Pintea. *Combinatorial optimization with bio-inspired computing.* PhD Thesis, Babes-Bolyai University, EduSoft Publisher, 2010.

[22] K. Scarfone and P. Mell. *Guide to Intrusion Detection and Prevention Systems (IDPS)*, 2007). `http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf`

[23] S. Selvakani and R. S. Rajes. Genetic algorithm for forming rules for intrusion detection. *Int. J. of Computer Science and Network Security* 7(11):285–290, 2007.

[24] R. Stoean, M. Preuss, C. Stoean, E. El-Darzi and D. Dumitrescu. Support Vector Machine Learning with an Evolutionary Engine. *J. Operational Research Society* 60(8):1116–1122, 2009.

[25] J. T. Yao, S. L. Zhao and L. V. Saxton. A study on fuzzy intrusion detection, SPIE, Data Mining, Intrusion Detection. Information Assurance and Data Networks Security, 5812:23–30, 2005.

[26] T. White. *Expert Assessment of Stigmergy.* A Report for the Department of National Defence. `http://www.scs.carleton.ca/~arpwhite/stigmergy-report.pdf`